

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method for calculating hashing of a message (FM) in a device communicating with a smart card, comprising:
 - storing a same hash function in said device and said smart card ~~storing the same hash function, wherein~~ the message ~~comprising~~ comprises data blocks including secret data (SD) and other public data (PD), and wherein secret data (SD) ~~being~~ is only known by the smart card[[,]];
 - performing ~~characterized in that the~~ a calculation of the hash function of the secret data (SD) ~~is performed~~ in the smart card; and
 - performing the calculation of the hash function of all or part of the other public data (PD) ~~is performed~~ in the device.
2. (Currently Amended) The method according to claim 1, ~~characterized in that~~wherein, if secret data (SD) is followed by the other public data (PD) in the message (FM), the smart card starts ~~calculating~~ the calculation of the hash function of all blocks that include a secret data (SD) and then sends the a corresponding intermediate result (R) to the (ME) device that continues ~~the hash calculation of the hash function~~ by using the intermediate result (R) and ~~the remaining other public data (PD)~~.
3. (Currently Amended) The method according to claim 2, ~~characterized in that~~wherein, if said [[H]] hash function hashes a the message block by block, and if a block of the message includes a part comprising secret data (SD) and another part comprising other public data (PD), the smart card ~~calculates~~ performs the calculation of the hash function of this block.
4. (Currently Amended) The method according to claim 1, ~~characterized in that~~wherein, if public data (PD) is followed by the other secret data (SD), the device (ME) starts ~~calculating~~ performing the calculation of the hash function of (PD) public data and then sends the corresponding intermediate result (R) and a remaining part (RP) of last hash block to the smart card that continues to ~~do~~ perform the calculation of the hash function ~~calculation~~

internally by using the intermediate result (R), the remaining part of last hash block, and the remaining secret data (SD).

5. (Currently Amended) An apparatus comprising:

a communication device (ME) being able configured to be coupled to a smart card (CAR), said device and said smart card storing the a same hash function;

the a message (MF) comprising data blocks including secret data (SD) and other public data (PD), wherein secret data (SD) being is only known by the smart card, characterized in that wherein said communication device includes a program for performing the following steps:

a hashing step in which all or part of said other public data (PD) are is hashed in said communication device, and

a requesting step in which, said communication system device requests the smart card to perform the hash function of all the secret data (SD).

6. (Currently Amended) An apparatus comprising:

A a smart card (CAR) coupled to a communication device (ME), said communication device and said smart card storing the a same hash function, the wherein a message (MF) comprising comprises data blocks including secret data (SD) and other public data (PD), wherein secret data (SD) being is only known by the smart card, characterized in that wherein said smart card includes a program for performing the following steps; when requested by the communication device (ME) as defined in claim 5, a step of hashing of all of said secret data (SD).

a hashing step in which all or part of said other public data is hashed in said communication device, and

a requesting step in which, said communication device requests the smart card to perform the hash function of the secret data.